STATEMENT OF WORK

Contract: N6600119D0058
Task Order: N6600120F1310
Date: Revised 19 January 2021
Title: NOBLE Software and Systems Engineering Services

1.0 SCOPE

The Department of Navy (DoN), Naval Information Warfare Center Pacific, (NIWC Pacific) is acquiring engineering services to support the Naval Warfare Center Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I), Command and Control (C2) Systems Program Office (PMW 150) Develop, Integrate, Field, and Sustain Naval Operations Business Logistics Enterprise (NOBLE) Integrated Data Environment.

The objective of this effort is to obtain the full range of technical and engineering services to assist and support NIWC Pacific to carry out its duties and responsibilities to support the delivery of the unclassified and classified Agile Warfighting Analytics Readiness Environment (AWARE) as well as to provide software and data integration for Navy Tactical Command Support Systems into the NOBLE family of systems. The range of services require subject matter expertise in specialized technology and engineering skill sets that match NIWC Pacific's requirements, to support operations and sustainment as well as software design and development. The operations and Sustainment support will include tasking for engineering management, Software Maintenance, Data Management, Systems Administration, and Cybersecurity. The software design and development support will include tasking for software design, software development, data engineering, data analysis, human factors design, and intergrade data environment administration.

This is a level of effort, severable task order.

1.1 Background

The NOBLE Family of Systems (FoS) increases Fleet readiness by improving operational availability, reliability, and sustainability across the Navy logistic support enterprise. These capabilities provide the ability to order/receipt/and stow parts, record ship and aviation maintenance actions, manage ship's store and food management, and perform various shipboard administrative functions.

AWARE is a proposed operational Cloud-hosted architecture and platform that will provide a multi-layer cloud and web-based implementation consisting of a Data as a Service (DaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) for shore based and deployed users. AWARE will provide application and data integration services to the Navy Operational Business Logistics Enterprise (NOBLE) Family of Systems (FoS), including the Naval Aviation Maintenance System, (NAMS), Naval Operational Maintenance Environment (NOME), and Naval Operational Supply System (NOSS). AWARE will also support other Logistics Information Technology Functional Area Manager (Log IT FAM) portfolio programs (e.g., USFF, PESTONI, ALE, MBPS, NMMES-TR). AWARE will enable automated software governance through Continuous Integration and Continuous Delivery (CI/CD) for the delivery acceptance, and authorization of commercial off the shelf software leveraging an end to end DEVOPs process. The current technical architectural solution is comprised of the Navy Research and Development Environment leveraging the Collaborative Software Amory. Additionally, AWARE will function as a data focused integrated platform, accessible via Application Program Interface (API) that will connect user applications, Data Lakes, and Enterprise Data Warehouses (EDW) in a distributed data environment. AWARE will incorporate common or customizable tools for analytics, such as: Extract, Transform, Load (ETL); Machine Learning (ML); Artificial Intelligence (AI); and Business Intelligence (BI) algorithms. AWARE will integrate the business systems, processes, and databases associated with creating and supporting curated data that will enable user access to actionable information. It will operate at cloud impact levels (IL) IL4, IL5 and IL6.

2.0 APPLICABLE DOCUMENTS

In the event of a conflict between the text of the SOW and the references cited herein, the text of this document shall take precedence. Nothing in this document, however, shall supersede applicable laws and regulations, unless a specific exemption has been obtained.

- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01I, 23 January 2015, Joint Capabilities Integration and Development System (JCIDS).
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01F, 21 March 2012, Net Ready Key Performance Parameter (NR KPP).
- Department of Defense Directive 8000.01, 10 February 2009, Management of the Department of Defense Information Enterprise.
- Department of Defense Directive 8570.01, 15 August 2004 (Certified Current as of April 23, 2007), Information Assurance Training, Certification, and Workforce Management.
- Department of Defense Instruction 8320.02, 5 August 2013, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense.
- Department of Defense 8320.2-G, 12 April 2006, Guidance for Implementing Net-Centric Data Sharing.
- Department of Defense Manual 5200.01, 24 February 2012, DoD Information Security Program.
- Department of Defense 5205.02-M, 03 November 2008, DoD Operations Security (OPSEC) Program Manual.
- Department of Defense 5220.22-M, February 2006, (Incorporating Change 1, 28 March 2013), National Industrial Security Program Operating Manual (NISPOM).
- Department of Defense 8570.01-M, 19 December 2005 (Incorporating Change 3, January 24, 2012), Information Assurance Workforce Improvement Program.
- Department of Navy, SECNAVINST 5000.36A, 19 December 2005, Department of the Navy Information Technology Applications and Data Management.
- Department of Navy, SECNAVINST 5230.14, 09 November 2009, Information Technology Portfolio Management Implementation.
- Department of Navy, SECNAV M-5239.2, 29 May 2009, Department of the Navy Information Assurance Workforce Management Manual to Support the IA Workforce Improvement Program.
- Department of Navy, SECNAVINST 5239.20, 17 June 2010, Department of the Navy Cybersecurity / Information Assurance Workforce Management, Oversight and Compliance.
- Department of Navy, SECNAVINST 5510.30B, 06 October 2006, Department of the Navy Personnel Security Program.
- Department of Navy, SECNAVINST 5510.36, 06 October 2006, Department of the Navy Information Security Program.
- Department of the Navy, SPAWARINST 3432.1, 02 February 2005, Operations Security Policy.
- ISO/IEC 12207:2008(E) (IEEE Std 12207-2008) Systems and Software Engineering-Software Life Cycle Processes.
- IEEE/EIA 12207.1-1997 IEEE Guide for Information Technology - Software Life Cycle Processes - Life Cycle Data.
- ISO/IEC 14764:2006(E) (IEEE STD 14764-2006) Software Engineering - Software Life Cycle Process – Maintenance.

3.0 PERFORMANCE REQUIREMENTS

3.1 NOBLE Operational Environment Support (NAVSEA OMN) – The purpose of this task is to support the implementation, integration and operational management of the NOBLE Agile Warfighting Analytics Readiness Environment for both Unclassified and Classified domains. The contractor shall assist the government with integrating and maintaining the operational cloud environment, supporting platforms, applications and data management.

3.1.1 Project Management– The contractor shall provide project management support to participate in demonstrations, meetings, working groups, and technical discussions related to the NOBLE Infrastructure, Platform, Integrated Data Environment, and FoS applications. The contractor shall work across the Integrated Product Team (IPT) Functional teams and with the program office to:

A) Document and maintain technical requirements for the NOBLE Enterprise Environment.
B) Create and maintain a NIWC Pacific Integrated Master Schedule to support the deployment of the NOBLE technical roadmap.

C) Document enterprise processes to perform, configuration management, requirements management, and risk Management.
D) Participate in Integrated Product Teams used to increase knowledge and understanding of the technical requirements for the deployment, integration, and configuration of NOBLE end products to the user.
E) Provide planning for acquisition support including the preparation of regulatory and statutory acquisition documentation.

3.1.2 Technical Management / Technical Writer– The contractor shall provide technical management, knowledge management, and technical writing support to maintain a variety of documentation and repositories to support information sharing to internal and external stakeholders. The contractor shall work with the IPT Functional teams and with the program office to:

A) Work with internal and external stakeholders to provide support for onboarding users and applications into the NOBLE environment,
B) Provide technical knowledge management for the development of technical documentation and systems operating procedures for interacting with the NOBLE Engineering Support team,
C) Develo a configuration management strategy that integrates the DevSecOps pipeline for Continuous Integration, Continuous Development, and Continuous Operations and Cybersecurity.
D) Assist the government in maintaining technical documentation, diagrams, and presentations pertaining to the NOBLE FoS to support cybersecurity, software design, and architecture development.
E) Assist in the preparation of the following documentations: Requirements Traceability Matrix, Integrated Master Schedule, Software\Data Design Description, Software\Data Product Specification, Software Version Description, System User Manual, and Software Build List.
F) Assist the government as an Agile SCRUM Master providing technical oversight for all Agile meetings and activities.

3.1.3 Software Engineering, Maintenance, and Application Support – The contractor shall provide application software maintenance support to assist with integrating vendor applications into the NOBLE Operational Enterprise Environment. The contractor shall provide full life cycle software engineering and network support. Specifically, in support of this task the contractor shall:

A) Assist the Government in deploying the NOBLE FoS in multiple security domains to include Non-Secure Internet Protocol Router (NIPR) and Secret Internet Protocol Router (SIPR) that are hosted in a Navy Operational Cloud environment.
B) Provide requirements analysis, software integration support, implementation and integration of software applications using open industry standard support software including but not limited to Redhat OpenShift, ElkStack, Forgerock, JFROG
C) Support the integration of unique customer-applications utilizing Java, Postgres, Palantir Foundry, as well as other software languages and technologies into the enterprise.
D) Provide full software life cycle system documentation and user training for each software application developed and implemented.
E) Maintain a repository of all current and past NOBLE baselines in all designated security domains.
F) Support DevSecOps through an automated pipeline hosted in the Collaborative Software Amory hosted in the NIWC Pacific NRDE Cloud environment.
G) Automate repetitive tasks creating scripts, and updating scripts in both Windows, Linux, and AWS environments. Familiarity with BASH, Powershell, Lambda, and Python scripting.
H) Monitor the deployment and operations of vendor applications to ensure system availability for end users and make recommendations for vendor application/network/system architecture changes to ensure end user system availably can be maintained.

3.1.4 Data Management– The contractor shall develop data management plans and procedures in support of net-centric solutions provisioned in a service-oriented architecture as well as interfacing with existing legacy NOBLE capabilities and networks. The contractor shall:

A) Manage the data pipeline to ensure requirements for ingesting and managing application data are identified.
B) Provide legacy application support to ingest data into the NOBLE Integrated Data Environment
C) Identify interface requirements to support existing and future access to the NOBLE Integrated Data Environment.
D) Design, build, test, deploy and support business intelligence solutions leveraging the NOBLE Integrated Data Environment using Palantir Foundry.
E) Develop and execute database queries and conduct analyses.
F) Develop and update technical documentation.
G) Support initiatives for data integrity and normalization.

3.1.5 Information Systems Management– The contractor shall provide systems administration and engineering design, technology upgrades, integration, operation, and maintenance of the NOBLE Enterprise Environment within the distributed information cloud infrastructure. This support includes all mission related servers (name, directory, messaging, application, web and collaboration), data storage, backup/recovery, software applications, platform services and operating systems required to enable robust and efficient information communications. Additionally, the contractor shall support initiatives enabling a more scalable, secure, containerized and adaptable infrastructure using methodologies focused on integrating security, development, and operations (SECDEVOPS) into a single continuous process. Specifically, in support of this task the contractor shall:

A) Configure Cloud Infrastructure, Virtual Private Clouds, Software Platforms, and supporting services.
B) Provide Cloud Infrastructure design, installation, configuration, testing, integration, life cycle recommendations, documentation, Defense Information Systems Agency (DISA) STIG applications, troubleshooting, repair, monitoring and management of enterprise network services and ACAS monitoring and compliance.
C) Provide installation, configuration changes, updates, and operation and maintenance of Enterprise Services required for the NOBLE Operational Environment to include Active Directory, Domain Naming Service, Backups, identity management, access control, logging, and monitoring.
D) In accordance with NOBLE requirements and DoD Cybersecurity directives, construct, harden, control and stage approved Operating System (O/S) load-configurations and containers for distribution to all NOBLE Vendors.
E) Provide design, installation, configuration, testing, integration, documentation, troubleshooting, repair, monitoring, and management of enterprise network services environments involving Microsoft Windows, Red Hat Linux, and Openshift installations.
F) Provide support that includes, but is not limited to, rapid deployment, analysis of information system usage and data flows, evaluation/installation of new Operating Systems (O/S), O/S software patches, and commercial application updates, documenting network services configuration changes.
G) Provide cybersecurity support to set up and resolve installation issues related to enterprise capabilities such as Host-based Intrusion Prevention System (HIPS), McAfee Firewall, Security Technical Implementation Guide (STIG) requirements, and Boundary change requests/Whitelist
H) Provide application integration support to troubleshoot and resolve issues for integrating applications into NOBLE Enterprise Services such as Structured Query Language (SQL) Databases, Postgres, Internet Information Server (IIS), RedHat Openshift, Apache, Group Policy, and Domain Name Server (DNS) etc.
I) Provide performance monitoring, troubleshooting, and resolve enterprise level issues with Wide Area Networking connectivity to include Secure Socket Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPsec) encryption, network and database connections across the WAN.

3.2 **NOBLE Cyber Security (PMW 150 OMN)** - The purpose of this task is to support the enterprise cybersecurity efforts for the certification, authorizations, and monitoring of the NOBLE Enterprise, Family of Systems. The contractor shall assist the government with providing technical support for the integration of various legacy applications into the operational NOBLE environment. Legacy NOBLE FoS include, but is not limited to NMRO (formerly NAMES, NOME), NOSS, NIDE, USFF PESTONI, NMMES-TR, and MBPS, etc.

3.2.1 Cyber Security RMF Support– The contractor shall assist the Government in maintaining ATO Cybersecurity Support for the PaaS, DaaS, and Application ATOs. This includes administrative, technical, and process orientated support. The contractor shall support cybersecurity efforts in a cloud environment supporting multiple operating environments to include Linux, Windows, Networking, AWS, application security, and DoD security assessment and hardening tools. The contractor shall:

A) Develop and maintain Assessment and Authorization (A&A) documentation, create and/or maintain all A&A documentation to include, but not limited to, Configuration Management (CM) baselines, Risk Management Framework (RMF) documentation, security reviews and assessments, Plan of Action and Milestones (POA&Ms), post accreditation documentation, and other security documents as required by the Navy's Authorization Official (NAO).

B) Manage the A&A effort. A&A must be performed in accordance with the latest DoD Instruction for RMF 8510. The contractor shall execute all steps necessary for obtaining accreditations and maintaining complete A&A packages for all assigned systems and platforms.

C) Initiate and track A&A meetings, maintain A&A meeting agendas, minutes and action items. All A&A documents shall be posted in a NOBLE designated controlled area.

D) Define security requirements,support evaluations and provide detailed recommendations on any current and new IT development efforts to ensure an efficient, successful A&A process.

3.2.2 Cyber Security Management and Monitoring Services – The contractor shall assist the government in deploying, configuring and managing the NOBLE Platform Virtual Data Center Management Services. Tasks include:

A) Running system scans, troubleshooting failed scans, configuring automated scans, configuring target systems, creating reports, analyzing results, and capable of remediating findings.

B) Installing, configuring, and troubleshooting Host Based Security System (HBSS) Electronic Policy Orchestrator, HBSS point products, create HIPS and firewall rules and exceptions, and understanding how to tune and maintain multiple operating systems running all required DoD products.

C) Providing integration, configuration, operation, management, monitoring, troubleshooting, and documentation in support of the Host Based Security System (HBSS) using McAfee ePolicy Orchestrator (ePO) for the NOBLE Enterprise Environment.

D) Installing, configuring, and troubleshooting the NOBLE DOD Assured Compliance Assessment Solution (ACAS) Solution in accordance with all DOD guidance and understanding how to tune and maintain multiple operating systems running all required DoD products.

E) Performing validation of cyber security controls in support of assessment and authorization efforts.

F) Providing security incident reports as required outlining the specific security issue, critical concerns, and remediation actions required to resolve or mitigate the issue.

3.3 NOBLE Systems and Software Engineering (NAVSEA RDTE) - The purpose of this task is to identify future requirements, design, and develop, technical solutions for NOBLE. This task includes providing development support for the integration of new capabilities into the NOBLE Platforms, Data services, as well as the development and analysis of various technical use cases to support Navy Maintenance, Repair, Overhaul, Supply and Logistics.

3.3.1 Software Design and Architecture Development – The contractor shall assist the government in developing a continuous integration / continuous development model to integrate NOBLE enterprise solutions, applications, and data requirements. Tasks include:

A) Defining full Stack development of software supporting the development of end to end continuous integrations / continuous delivery of COTS applications.
B) Translating user requirements into an overall architecture and implement new systems to support the automation of delivery, acceptance, testing, and delivery of software and data solutions for NOBLE.
C) Supporting analysis of requirements impacting system deployment and delivery (e.g. Network throughput constraints, deployment site capabilities, Navy Cloud Brokerage capabilities, etc.) and identify risks, issues, solutions, and system architectures to meet those requirements.
D) Providing NOBLE SW SME Support for data driven applications to support NMRO and Logistics.
E) Performing requirements modeling using MBSE (model-based system engineering) techniques and tools to ensure all requirements are captured, ensure enterprise/solution/system architectures meet those requirements, and ensure all work traces to the requirements.
F) Defining use cases and prioritize requirements in support of project managers building product backlogs for teams to execute work. Identify dependencies between teams executing work to meet requirements and identify tools/architectural solutions and define processes/procedures to streamline work execution.
G) Supporting enterprise working groups working to resolve complex portfolio level multi-disciplinary engineering problems affecting the deployment and operations of the NOBLE Family of Systems.

3.3.2 Software Development– The contractor shall assist the government in creating software applications, dashboards, and readiness aids to support NOBLE stakeholders. Tasks include:

A) Designing, developing and testing simple to moderate Palantir Foundry dashboards and data visualizations leveraging both established guidelines and custom designs and the ability to create formulas and calculations to meet the needs of business logic.
B) Designing, developing, and testing simple to moderate reports using Palantir Foundry
C) Be an active participant in the development of the overall reporting roadmap.
D) Interacting cross-functionally with a wide variety of people and teams. The contractor shall work closely with analysts and data engineers to identify opportunities and assess improvements of NOBLE solutions.
E) Producing and maintain accurate project documentation.

3.3.3 Data Engineering– The contractor shall assist the government in developing a NOBLE data pipeline to align data requirements with NOBLE requirements for data acquisition, data driven processes, data analysis and task automation. Tasks include:

A) Creating and maintaining data pipelines and advanced analytics that capture data for NMRO and SCM purposes
B) Building out the data pipelines and scripting. Using Python
C) Data and API Integrations [REST, SOAP, etc]
D) Providing data ingestion, processing, and storing large and diverse datasets.

3.3.4 Data Analysis–The contractor shall assist the government for leveraging the NOBLE IDE to prepare data for predictive and prescriptive modeling and leverage data analytics, machine learning, and statistical methods to identify data patterns to improve Navy Maintenance Repair, and overhaul. Tasks include:

A) Identifying new sources of data and methods to improve data collection, analysis, and reporting in NOBLE DaaS.
B) Collaborating with stakeholders and obtain buy-in by providing easy-to-understand explanations of data analysis through reports and visual dashboards that deliver high-value insights
C) Designing algorithms and data manipulation capabilities using R, Python, C++, JavaScript, Go, and other known programming languages.

D) Building data solutions, tools, and capabilities to enable self-service frameworks for data consumers to monitor and report on data.
E) Improving the quality of data use and usability by driving an understanding and adherence to the principles of data quality management including metadata, lineage, and business definitions

3.3.5 User Interface (UI) Design–The contractor shall assist the government in designing NOBLE UIs that support Fleet needs for Fleet needs for data driven applications to support advanced information sharing and decision making support. The contractor shall:
A) Participate in user engagement activities for the purpose of capturing user feedback and translating user needs into designs
B) Design high-converting, user-friendly experiences across multiple NMRO and SCM solutions.
C) Develop UI mockups and/or interactive prototypes with tools such as Photoshop, Illustrator, Sketch, Omnigraffle, Keynote, Axure, Balsamiq, InVision, and/or similar industry-level design and prototyping applications
D) Create designs from scratch or make updates to existing designs that can be used for client deliverables
E) Produce as-is and to-be user flows, sitemaps, and wireframes
F) Work closely with the development team to ensure designs are fully implementable
G) Ensure all designs are built on a foundation of solid usability and intuitive design principles
H) Leverage analytics data as a basis for UX problem resolution

3.3.6 DaaS Administration– The contractor shall assist the government in the design and configuration of the NOBLE Integrated Data Environment Data as a Service. The DaaS solution is a Big Data solution provided Software as a Solution service hosted in Amazon Web Services in the DISA Provided Gov Cloud using Palantir Foundry. Tasks include:
A) Providing Palantir cloud infrastructure based on AWS EC2 and S3
B) Designing, implementing, and unit testing query optimization features for Palantir Foundry database software leveraging agile and continuous delivery methodologies.
C) Designing and reviewing architectures and design to optimize query features and recommend enhancements.
D) Working closely with DaaS vendor Customer Support team to provide technical guidance to implement customer data solutions.

3.4 **NOBLE DevSecOps Engineering** (PMW150 RDT&E) – The purpose of this task is to support DevSecOps engineering for the NOBLE Enterprise, which includes the research, design, development, implementation, integration, testing, monitoring, and cybersecurity considerations for NOBLE applications and frameworks. The contractor shall assist the government with providing technical support for all aspects of DevSecOps engineering, leveraging the Collaborative Software Armory (CSA) hosted on NIWC Pacific's Navy Research and Development Environment (NR&DE) cloud platform. Tasks Include

A) DevSecOps Research and Design – The contractor shall assist with the research and design of continuous integration / continuous delivery (CI/CD) pipelines through automated solutions. The overall design should consider software builds, application hosting, application deployment, functional testing, penetration testing, static code analysis, release management, and environment integration.
B) DevSecOps Development and Integration – The contractor shall assist with the development and integration of CI/CD pipeline tools and underlying infrastructure. This includes integrating NOBLE applications into CSA and NR&DE for software builds, application hosting, application deployment, functional testing, penetration testing, static code analysis, release management, and environment integration.

4.0 ESTIMATED TRAVEL

The following table represents estimated long distance travel requirements for the base period in support of this task order. All travel is expected to originate from the San Diego, CA area.

Destination	# of Trips	# of People	# of Days	SOW Para.
Norfolk, VA	2	1	5	3.1
Arlington, VA	2	1	5	3.1
Norfolk, VA	2	1	5	3.2
Arlington, VA	2	1	5	3.2
Norfolk, VA	2	1	5	3.3
Arlington, VA	2	1	5	3.3

5.0 PROPERTY REQUIREMENTS

Government Furnished Property (GFP) is not anticipated at this time.
Government Furnished Information (GFI) is not anticipated at this time.
Government Property (Incidental) is anticipated for work at Government site (e.g. contractor access to NIWC work stations while working on Government site only).
Government Furnished Facilities shall be made available (e.g. accessing Government facility for SOW performance).
Contractor Acquired Property (CAP) is not anticipated at this time.

6.0 Security

The security requirement for this tasking will be up to and including Secret. The work performed by the contractor will include access to unclassified and up to Secret data, information, meetings, and spaces. The contractor may require access to Secure Internet Protocol Router Network (SIPRNet). The contractor shall receive the North Atlantic Treaty Organization (NATO) awareness brief and complete the derivative classification training prior to being granted access to SIPRnet; training is provided by the facility security officer. This briefing is not entered into the Joint Adjudication Personnel System (JPAS). Evidence of completion, training certificates or equivalent, shall be provided to the NATO Control Officer when requested. The contractor shall not use the SIPRNET for anything except that which is required for this contract.
Anti-Terrorism/force Protection **(AT/FP)** briefings are required to be completed annually for all personnel (military, DOD civilian, and contractor). The briefing is available at Joint Knowledge Online (JKO): https://jkodirect.jten.mil (prefix): JS; course number: US007; title: Level 1 Anti-terrorism awareness training, if experiencing problems accessing this website contact the JKO Help Desk (24 hours a day/7 days a week, jkohelpdesk@jten.mil, 757-203-5654). The website will allow contractors who do not have a CAC to access the training. note: per OPNAVINST F3300.53C contractor employees must receive the AT/FP briefing annually.
As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on:

(1) the status of the facility clearance (FCL);
(2) the status of an employee's personnel clearance (PCL); the status of an employee's personnel clearance (PCL); may indicate the employee poses an insider threat;
(3) the proper safeguarding of classified information;
(4) or an indication that classified information has been lost or compromised.

Contractors working under NIWC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the COR/TPOC, the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or DODCAF when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under NIWC Pacific contracts.

7.0 DATA DELIVERABLES

Data deliverables shall be reviewed in accordance with the Department of the Navy Policy on Digital Product/Technical Data, Assistant Secretary of the Navy for Research, Development and Acquisition, ASN (RDA), memo of 23 October 2004, and as specified in the Contract Data Requirements List (CDRL) attachment for this task order.

SOW ADDENDUM

I. KEY PERSONNEL

(a) The offeror agrees to assign to this contract those key personnel listed in paragraph (d) below. No substitutions shall be made except in accordance with this text.

(b) The offeror agrees that during the first 120 days of the contract performance period no personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death or termination of employment. In any of these events, the contractor shall promptly notify the Contracting Officer and provide the information required by paragraph (c) below. After the initial 120 day period, all proposed substitutions must be submitted in writing, at least fifteen (15) days (thirty (30) days if a security clearance is to be obtained) in advance of the proposed substitutions to the contracting officer. These substitution requests shall provide the information required by paragraph (c) below.

(c) All requests for approval of substitutions under this contract must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute or addition, and any other information requested by the Contracting Officer or needed by him to approve or disapprove the proposed substitutions. All substitutions proposed during the duration of this contract must have qualifications of the person being replaced. The Contracting Officer or authorized representative will evaluate such requests and promptly notify the contractor of approval or disapproval thereof in writing.

(d) List of Key Personnel

NAME	CONTRACT LABOR CATEGORY
Jason Mak (FSI)	Program Manager
Max Geiszler (FSI)	Senior Computer Scientist
Himanshu Buha (FSI)	Computer Scientist
Marley Pucket (KPMG)	Technical Writer

(e) If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the contract work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate. In addition, if the contractor is found at fault for the condition, the Contracting Officer may elect to equitably decrease the contract price or fixed fee to compensate the Government for any resultant delay, loss or damage.

(f) If the offeror wishes to add personnel to be used in a labor category, it shall employ the procedures outlined in paragraph (c) above. Adding personnel will only be permitted in the event of an indefinite quantity contract, where the Government has issued a delivery order for labor hours that would exceed a normal forty hour week if performed only by the number of employees originally proposed.

II. TECHNICAL DIRECTION

(a) Technical Direction may be provided to the contractor from time to time by the Contracting Officer or Contracting Officer's Representative, if authorized, during the term (term is defined as the period of performance for the basic contract and any options that may be exercised) of this contract. Technical Direction will provide specific information relating to the tasks contained in the Statement of Work and will be provided to the contractor in writing. Any Technical Direction issued hereunder will be subject to the terms and conditions of the contract. The contract shall take precedence if there is any conflict with any Technical Direction issued hereunder, and cannot be modified by any Technical Direction.

(b) As stated, Technical Direction shall be issued in writing and shall include, but not be limited to:

(1) date of issuance of Technical Direction;
(2) applicable contract number;
(3) technical direction identification number;
(4) description of Technical Direction;
(5) estimated cost;
(6) estimated level of effort by labor category; and
(7) signature of the PCO or COR.

(c) If the contractor does not agree with the estimated cost specified on the technical direction, or considers the technical direction to be outside the scope of the contract, it shall notify the PCO or COR immediately and, in the case of the estimated cost, arrive at a general agreement to the cost of the task. In the case of the direction requiring work that is out of the scope of the contract, the contractor shall not proceed with the effort unless and until the PCO executes a contract modification to include the change in scope.

III. REPORTING REQUIREMENTS FOR CONTRACTED SERVICES

Services Contract Reporting (SCR) requirements apply to this contract. The contractor shall report required SCR data fields using the SCR section of the System for Award Management (SAM) at following web address: https://sam.gov/SAM/.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://sam.gov/SAM/.

IV. CYBERSECURITY

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

Cyber IT and Cybersecurity Personnel

(a) The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

(b) The contractor shall be responsible for identifying, tracking and reporting cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Although the minimum frequency of reporting is monthly, the task order can require additional updates at any time.

(c) Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in para 8.2.2.4(b).

When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g., .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Pacific Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the NIWC Pacific IAM office. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.
2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the NIWC Pacific IAM office or from the website: https://navalforms.documentservices.dla.mil/.

(d) Contractor personnel with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum:

Acceptable Use of Department of the Navy Information Technology (IT) dated 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in para 5.2.2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

Cybersecurity Workforce (CSWF) Report

DoD 8570.01-M and DFARS PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report as applicable at the task order level. IAW DFARS clause 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided at the task order level, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

Information Technology (IT) Services Requirements

This paragraph only applies to IT contracts. Information Technology (IT) is defined as any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data of information by the agency. IT includes computers, ancillary equipment, peripherals, input, output, and storage devices necessary for security and surveillance. Electronic and Information technology (EIT) is IT that is used in the creation, conversion, or duplication of data or information. EIT includes: telecommunication products, such as telephones; information kiosks; transaction machines; World Wide Web sites; multimedia (including videotapes); and office equipment, such as copiers and fax machines.

Information Technology (IT) General Requirements

When applicable, the contractor shall be responsible for the following:

• Ensure that no production systems are operational on any RDT&E network.
• Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.
• Migrate all Navy Ashore production systems to the NMCI environment where available.
• Work with government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).
• Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.
• Register any contractor-owned or contractor-maintained IT systems utilized on contract in the Department of Defense IT Portfolio Registry (DITPR)-DON.
• Only perform work specified within the limitations of the task order.

Acquisition of Commercial Software Products, hardware, and Related Services

This paragraph only applies to the purchasing/hosting of commercial software. Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

DON Enterprise Licensing Agreement/DOD Enterprise Software Initiative Program

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dated 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and government-wide SmartBuy program (see DoD memo dated 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the task order level.

DON Application and Database Management System

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

Section 508 Compliance

This paragraph only applies to IT contracts. The contractor shall ensure that all software recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, 26 CFR Part 1194 and pursuant to SPAWARINST 5721.1B of 17 Nov 2009. In accordance with FAR 39.204, this requirement does not apply to

contractor acquired software that is incidental to the task, software procured/developed to support a program or system designated as a National Security System (NSS) or if the product is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment.

Software Development/Modernization and Hosting

This paragraph only applies to software development and modernization. The contractor shall ensure all programs utilizing this contract for software development/ modernization (DEV/MOD), including the development of IT tools to automate NIWC Pacific business processes are compliant with DON Information Management/Information Technology (DON IM/IT) Investment Review Process Guidance requirements. Contractors shall neither host nor develop IT tools to automate NIWC Pacific business processes unless specifically tasked within the task order or contract. The contractor shall ensure IT tools developed to automate NIWC Pacific business processes will be delivered with full documentation and source code, as specified at the task order level, to allow non-proprietary operation and maintenance by any source. The contractor shall ensure all programs are submitted with proof of completed DEV/MOD certification approval from the appropriate authority in accordance with DON policy prior to task order award. *Note must be listed on Investment Review Board (IRB) approved list.

Information Security

Pursuant to DoDM 5200.01 and DoD 5200.48, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

IT Position Designations

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of Special-Sensitive (SS)/Critical-Sensitive (CS) or Noncritical Sensitive (NCS), access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Per SECNAVINST 5510.30C, page 7, Section 8.b of enclosure (4), the Information Systems Security Manager is responsible for establishing, implementing and maintaining the DoN information system and information assurance program and is responsible to the Commanding Officer for developing, maintaining, and directing the implementation of the Information Assurance (IA) program within the command. The three basic position sensitivity levels/Position Designations:

Special-Sensitive (SS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for inestimable impact and/or damage.

Critical-Sensitive (CS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for grave to exceptionally grave impact and/or damage.

Noncritical Sensitive (NCS)/T3 or T3R; equivalent (ANAC/ANACI) (IT Level II) - Potential for some to serious impact and/or damage.

V. INTELLIGENCE OVERSIGHT

For any contractor personnel conducting Intelligence or Intelligence-related activities or supporting those efforts under Department of Defense authorities shall report any Questionable Intelligence Activity (QIA), Significant, or Highly Sensitive Matter (S/HSM) to the Naval Information Warfare Systems Command Intelligence Oversight Program Manager or Senior Intelligence Officer.

Questionable Intelligence Activity (QIA): Any Intelligence or Intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

Significant or Highly Sensitive Matter (S/HSM): An Intelligence or Intelligence-related activity (regardless of whether the Intelligence or Intelligence-related activity is unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by Intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of Intelligence activities. Such matters might involve actual or potential:

- Congressional inquiries or investigations
- Adverse media coverage
- Impact on foreign relations or foreign partners

Systemic compromise, loss, or unauthorized disclosure of protected information

VI. CONTRACTOR FURNISHED EQUIPMENT ON RDT&E NETWORKS

Contractors are prohibited from connecting any non-Government owned equipment to RDT&E networks unless the equipment is specifically identified hereunder. The following contractor owned/provided equipment is permitted to be connected to the RDT&E network, as necessitated by the statement of work, in performance of this contract only:

- Contractor Owned Laptop Computers – Reimaged with RDT&E approved images

Any changes to this list must be completed via formal contract modification prior to implementation or use on the network. Before connection of any above-listed equipment is made, the Command Information System Security Manager (Code 82400) must be informed via Cybersecurity Exception Request. All other equipment not specifically identified above remains prohibited for use on RDT&E networks.

Per the DON Destruction of Electronic Storage Media Policy, all contractor-provided internal and removable electronic storage media listed above shall become Government property upon the sooner of: equipment end of life, replacement, end of service, or turn-in; contract completion, or contract termination. The contractor shall work with the Contracting Officer or Contracting Officer's Representative (COR), if applicable, to facilitate the immediate turnover of internal and removable electronic storage media as soon as one of the aforementioned circumstances arise.

Internal and removable electronic storage media includes, but is not limited to, workstations, laptops/notebooks, printers, copiers, scanners, multi-functional devices (MFD), and hand held devices with internal storage devices, removable hard drives, external hard drives, solid state hard drives, flash based storage media such as "thumb" drives and camera memory cards, backup data systems (e.g., DAT, LTO, DLT), and optical storage devices (e.g., CD/DVD).